УДК 004.056.5-047.58

А.С. Шабуров[1], С.А. Юшкова[1], А.В. Бодерко[2]

[1]Пермский национальный исследовательский политехнический университет, Пермь, Россия
[2]ЗАО «Бионт», г. Пермь, Россия

МОДЕЛИРОВАНИЕ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Решение задачи оценки угроз безопасности для различных информационных систем является основой для применения необходимых методов и средств защиты информации. Качественная оценка позволяет решать проблему информационной безопасности наиболее эффективно. В статье анализируются существующие подходы к оценке угроз безопасности информационных систем персональных данных на основе действующих методик. Процесс оценки угроз информационной безопасности осуществляется с учетом исследования исходного состояния защищенности информационной системы и вероятностных характеристик действий нарушителя. Приводятся примеры практического применения действующих нормативно-правовых документов, раскрываются методические подходы по совершенствованию применения данных подходов по обоснованию и оценке рисков информационной безопасности. Предлагается концептуальный подход по оптимизации процесса анализа угроз информационной безопасности, обосновывается целесообразность использования алгоритмов объектного программного моделирования, позволяющих оптимизировать процедуры оценки угроз, на основе разработки соответствующей системы информационно-аналитической поддержки.

Ключевые слова: угроза безопасности, информационная система, защита информации, персональные данные, оценка риска, система информационно-аналитической поддержки.

A.S. Shaburov[1], S.A. Yushkova[1], A.V. Boderko[2]

[1]Perm National Research Polytechnic University, Perm, Russian Federation
[2]«Biont» closed joint-stock company

MODELLING OF EVALUATION OF SECURITY THREATFOR INFORMATIONAL SYSTEMS DEALING WITH PERSONAL DATA

Solving the problem of evaluation of security threat for different informational systems is the basis for necessary information security methods and means application. Qualitative evaluation allows solving the problem of information security in the most effective way. Current approaches to evaluation of security threat for informational systems dealing with personal data based on actual methodologies are being analyzed in the article. The process of security threat evaluation is conducted considering examination of initial information system security state and probabilistic characteristics of intruder's actions. Some practical appliances of current regulatory documents are given as examples. Some methodological approaches to improvement of appliance of these approaches on informational security risks justification and evaluation. Conceptual approach to optimization of the process of informational security threat analysis has been suggested. The appropriateness of objective programming modelling algorithm usage has been proved in the article. These algorithms allow optimizing threat evaluation procedure based on the development of adequate informational analytical support system.

Keywords: security threat, informational system, information security, personal data, evaluation of risks, informational analytical support system.

В настоящее время достаточно актуальной является задача оценки угроз информационной безопасности для различных информационных систем. Проведение качественной оценки становится основой для применения необходимых методов и средств защиты информации и позволяет решать данную проблему наиболее эффективно. Традиционно определение требований как по защите информации, так и по оценке угроз безопасности информации осуществляется на основе правового и нормативно-методического обеспечения.

Например, Законом №152-ФЗ «О персональных данных» для операторов, использующих в своей деятельности информационные системы персональных данных, установлена обязанность принимать необходимые меры по обеспечению их безопасности. В свою очередь обеспечение безопасности персональных данных (ПДн) достигается, в частности, определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИС ПДн) [1].

Для решения задач построения моделей угроз операторам ПДн предлагается перечень нормативно-методических документов, в общем обеспечивающий процесс построения частных моделей угроз информационной безопасности в ИС ПДн [2, 3]. При этом сохраняются определенные ограничения на моделирование, связанные с разнообразием ИС ПДн, разновидностями факторов воздействия на информацию, что не всегда позволяет адекватно и всесторонне произвести оценку той или иной угрозы.

Для полноценной и адекватной оценки угроз требуется совершенствование подходов к применению действующих методик, базирующееся на опыте их реализации и традиционных технологиях построения частных моделей угроз информационной безопасности.

Обычно представление о природе воздействия угрозы безопасности на информационные ресурсы включает в себя определенный перечень составляющих компонентов, необходимых и достаточных для создания адекватной модели. К данному перечню компонентов, приведенному на примере ИС ПДн, относится следующая информация:

– об источниках угроз безопасности информации;

– о характерных угрозах безопасности информации;

– о способах реализации угрозы (атаки на информационные ресурсы);

– об уязвимостях информационной системы;

– о характере (категории) обрабатываемой информации.

На рис. 1 представлена модель реализации угрозы безопасности информации в ИС ПДн на основе вышеперечисленных исходных данных, в свою очередь получаемых из материалов статистических данных, по результатам научных исследований информационных систем или определенных специальными перечнями.

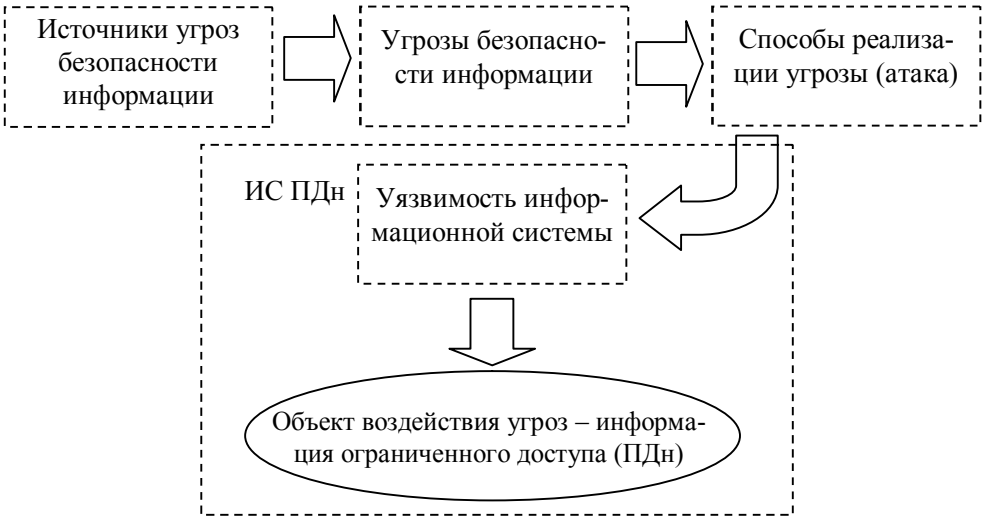

Рис. 1. Модель реализации угрозы безопасности информации в ИС ПДн

Правильно разработанная модель угроз ИС ПДн позволит в дальнейшем подобрать оптимальные технические и организационные меры по защите информации, создать эффективную систему защиты. В то же время неадекватная модель может не учесть существенные угрозы и привести как к неоправданным затратам материальных и финансовых ресурсов, так и утрате конфиденциальности, целостности и доступности самой информации ограниченного доступа.

Для упрощения процедуры моделирования угроз безопасности ИС ПДн на практике используются методические рекомендации специальных служб (ФСТЭК России, ФСБ России), регулирующих и контролирующих вопросы защиты ПДн, в соответствии с действующим российским законодательством. При этом каждые из рекомендаций имеют свои отличительные особенности.

Методические документы ФСТЭК России в основном ориентированы на составление модели угроз информационной системы, недостаточно учитывая фактор разнообразия вероятного поведения нарушителя. Методические рекомендации ФСБ России, наоборот, в большей степени ориентированы на модель нарушителя и не в полной мере учитывают модель угроз информационной системы.

Практическое применение вышеназванных методик позволяет сделать вывод о возможности их совместного использования с целью построения адекватной модели угроз безопасности ИС ПДн.

Для вероятностной оценки действий нарушителя целесообразно в соответствии с [2] определить шесть их основных типов: Н1, Н2, ... , Н6. При этом возможности нарушителя типа H_{i+1} включают в себя возможности нарушителя типа H_i, где $1 \le i \le 5$, а для отдельных типов нарушителей можно выделить отличительные признаки, приведенные в таблице.

Возможности нарушителей

Тип нарушителя	Информация об объекте атаки	Средства атаки	
		Чем располагают	Как использовать
Н1		Доступные в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные криптосредства только за пределами КЗ
Н2		=	Используют штатные средства в зависимости от орг. мер
Н3	Известны все сети связи, работающие на едином ключе	= + дополнительные средства в зависимости от орг. мер.	=
Н4	=	=	= + проводят лаб. анализ криптосредств
Н5	= + имеют исходные тексты прикладного ПО	=	=
Н6	=	безграничный доступ	=

Знаком «=» в таблице обозначены условия информационной атаки, соответствующие предыдущему типу нарушителя, а знаком «+» – вновь появляющиеся условия.

Далее осуществляется классификация нарушителей по признаку принадлежности и по возможности осуществлять атаки на ИСПДн, а также их категорирование с точки зрения вероятного воздействия. Проанализированный вид нарушителя, исходя из степени знания об объекте атаки, доступных ему средствах атаки, необходимо соотносится с типами нарушителей.

Например, администратору ИС ПДн известны все сети связи, работающие на едином ключе, но он не обладает испытательной лабораторией и исходным кодом программы, следовательно, его можно отнести к классу Н3. При этом таких сотрудников, как администратор безопасности или системный администратор, необходимо подбирать из числа доверенных лиц, а следовательно, их можно исключить из числа наиболее вероятных нарушителей.

Таким образом, присвоив каждому из выявленных вероятных нарушителей соответствующий тип и исключив лиц, которые не могут выступать в роли вероятных нарушителей, становится возможным определить необходимый уровень криптозащиты в ИС ПДн.

Несомненным достоинством предложенной методики является оценочная шкала, позволяющая с заданным ограничением, приемлемым для процедуры моделирования, произвести вероятностную оценку действий нарушителя, дать наиболее адекватную оценку угрозы «человеческого фактора».

Выявление актуальных угроз для информационной системы, основанное на методических рекомендациях ФСТЭК России, позволяет на первоначальном этапе существенно ограничить набор опасных факторов, воздействующих на информацию, а на следующем этапе оценить каждую из угроз безопасности информации с точки зрения их вероятности возникновения и степени опасности от последствия реализации.

Например, при выявлении угроз несанкционированного доступа для информации, передаваемой по каналам связи в распределенных ИС ПДн, таковыми угрозами могут быть:

– угроза «анализ сетевого трафика» с перехватом передаваемой из ИС ПДн и принимаемой из внешних сетей информации;

– угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих

станций ИС ПДн, топологии сети, открытых портов и служб, открытых соединений;

– угрозы выявления паролей по сети;

– угрозы навязывания ложного маршрута сети;

– угрозы подмены доверенного объекта сети;

– угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

– угрозы типа «отказ в обслуживании»;

– угрозы удаленного запуска приложений;

– угрозы внедрения по сети вредоносных программ.

Данный список необходимо дополнить перечнем угроз, которые могут быть актуальны для конкретной ИС ПДн в реальных условиях эксплуатации. Например, если в ИСПДн используется технология виртуализации серверов или рабочих станций, то можно дополнительно выделить следующие угрозы в виде атак:

– на гипервизор с виртуальной машины;

– на диск виртуальной машины;

– на средства администрирования;

– на виртуальную машину с другой виртуальной машины.

Формирование полного набора характерных угроз для конкретной ИС ПДн позволяет перейти к оценке актуальности каждой из них.

В данном случае считается целесообразным придерживаться традиционной последовательности оценки, последовательно определяя следующие характеристики системы: уровень исходной защищенности ИС ПДн, вероятность реализации угрозы, коэффициент реализации угрозы, показатель опасность угрозы. В заключение необходимо сделать вывод об актуальности угрозы.

Уровень исходной защищенности устанавливается на основании заранее разработанных критериев – характеристик информационной системы (режим обработки информации, распределенность ресурсов и т.п.), существенных с точки зрения защищенности ПДн, и оценивается общим коэффициентом. При этом определенный критериальный набор исходных данных значительно упрощает взгляд на реальную информационную систему, но может отрицательно повлиять на качество и адекватность оценки.

При осуществлении вероятностной оценки каждой из угроз рекомендуется использование заранее разработанной оценочной методики:

1) малая вероятность – вид угрозы не актуален для ИСПДн ввиду отсутствия данного вида обработки ПДн, либо разработан полный комплект организационно-распорядительных документов и внедрены сертифицированные технические средства защиты информации, полностью исключающие данную угрозу;

2) низкая вероятность – существуют объективные посылки для реализации угрозы, но разработаны и внедрены организационные меры, причем средства защиты не прошли сертификацию, либо имеются незначительные недочеты в системе защиты;

3) средняя вероятность – существуют объективные предпосылки для реализации угрозы, защитные меры внедрены, но имеются значительные недоработки;

4) высокая вероятность – существуют объективные предпосылки для реализации угрозы, защитные меры не внедрены.

Итоговый коэффициент реализуемости угрозы Y рассчитывается по формуле

$$Y = \frac{(Y_1 + Y_2)}{20},$$

где Y_1 – уровень исходной защищенности ИС ПДн; Y_2 – вероятность реализации конкретной угрозы.

Для определения степени опасности угрозы также следует применять принцип разделения их по уровням, исходя из результатов и последствий информационной атаки, например:

1) низкая опасность – реализация угрозы приводит к незначительным негативным последствиям;

2) средняя опасность – реализация угрозы приводит к негативным последствиям;

3) высокая опасность – реализация угрозы приводит к значительным негативным последствиям.

Результатом проведенных исследований считается полный набор актуальных угроз безопасности для ИС ПДн, составляющий основу частной модели нарушителя.

В конечном итоге реализация методики оценки угроз и построение частной модели угроз безопасности ИС ПДн заключаются в последовательном выполнении следующих процедур:

– вероятностная оценка действий нарушителя в среде ИС ПДн;

– определения перечня характерных угроз ИС ПДн на основе базовой модели;

– оценка исходной защищенности ИС ПДн с использованием определенных критериев оценки;

– определение вероятностной оценки угрозы ИС ПДн;

– определение степени опасности реализации угрозы;

– вывод об актуальности (неактуальности) угрозы на основании технологии оценки риска.

Расчет и оценки риска, как правило, осуществляются на основании универсальной методики, основанной на определении следующих параметров: A – стоимость ресурса – величина, характеризующая его ценность для решения основной задачи ИС; E – мера уязвимости ресурса по отношению к рассматриваемой угрозе; P – оценка вероятности реализации угрозы (как правило, за определенный период времени); S_1 – оценка ожидаемого возможного ущерба от единичной реализации определенной угрозы, определяемая по формуле

$$S_1 = A \cdot E;$$

где S_{sum} – итоговые ожидаемые потери от конкретной угрозы за определенный период времени, т.е конечная величина оценки риска, определяемая по формуле

$$S_{\text{sum}} = S_1 \cdot P.$$

На заключительном этапе оценки угроз целесообразно использование алгоритмов объектного программного моделирования [4], позволяющих оптимизировать процедуры оценки, на основе разработки системы информационно-аналитической поддержки (рис. 2).

Кроме того, для экспериментального подтверждения достоверности проведенной оценки целесообразно использование специально разработанных программных продуктов: «Ревизор Сети 2.0», «XSpider», «Terier», «ФИКС» и т.п.

Таким образом, требования по защите информационных систем персональных данных во многом определяются качеством и адекватностью процедуры оценки угроз информационной безопасности. Оценка угроз информационной безопасности предусматривает как исследование исходного состояния защищенности информационной системы, так и расчет вероятностных показателей действий нарушителя и возможности самой угрозы.

Рис. 2. Алгоритм программного моделирования оценки угроз информационной безопасности

Степень опасности угрозы определяется оценкой результата ее реализации, что позволяет произвести расчет риска. Использование алгоритмов объектного программного моделирования на основе разработки системы информационно-аналитической поддержки оптимизирует процедуры оценки, позволяет осуществлять моделирование как самих угроз информационной безопасности, в частности, так и систем защиты информации в целом.

Библиографический список

1. Федеральный закон от 27 июля 2006 г. № 152-фз «О персональных данных» // Российская газета. – 29 июля 2006. – № 4131.

2. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ РФ 21.02.2008 № 149/54-144) [Электронный ресурс]. – URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=126992 (дата обращения: 15.07.2013).

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. замдиректора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс]. – URL: http://fstec.ru/normativnye-i-metodicheskie-dokumenty-tzi/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения: 15.07.2013).

4. Бузинов А.С., Жигулин Г.П., Шабаев Р.И. Моделирование и прогнозирование информационных угроз как составная часть Концепции информационной безопасности РФ // Известия Российской академии ракетных и артиллерийских наук. – 2010. – № 4(66) [Электронный ресурс]. – URL: http://faculty.ifmo.ru/ikvo/MPES/downloads/modinfygr.doc (дата обращения: 15.07.2013).

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Юшкова Светлана Алексеевна (Пермь, Россия) – студентка кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: s.yushkova@mail.ru).

Бодерко Андрей Викторович (Пермь, Россия) – ведущий специалист по защите информации ЗАО «Бионт» (614015, ул. Красснова, д. 24, e-mail: info@biont.ru).

About the authors

Shaburov Andrey Sergeevich (Perm, Russian Federation) is PhD of Technical Sciences at the Department of Automation and Telemechanics, Perm National Research Polytechnic University (614990, 29, Komsomolsky prospect, Perm, e-mail: shans@at.pstu.ru).

Yushkova Svetlana Alexeevna (Perm, Russian Federation) is a student of the Department of Automation and Telemechanics, Perm National Research Polytechnic University (614990, 29, Komsomolsky prospect, Perm, e-mail: s.yushkova@mail.ru).

Boderko Andrey Viktorovish (Perm, Russian Federation) is the Leading Expert on informational security at «Biont» closed joint-stock company (614015, 24, Krasnova st., Perm, e-mail: info@biont.ru).

Получено 05.09.2013